

# SAP SECURITY



**tutorialspoint**

SIMPLY EASY LEARNING

[www.tutorialspoint.com](http://www.tutorialspoint.com)



<https://www.facebook.com/tutorialspointindia>



<https://twitter.com/tutorialspoint>

## About the Tutorial

---

SAP Security is required to protect SAP Systems and Critical Information from Unauthorized Access in a Distributed Environment while accessing the system locally or remotely. It covers various Authentication Methods, Database Security, Network and Communication Security and protecting standard users and other best practices that should be followed in maintaining your SAP Environment.

In a SAP Distributed Environment, there is always a need that you protect your critical information and data from unauthorized access. Human Errors, Incorrect Access Provisioning shouldn't allow unauthorized access to system and there is a need to maintain and review the profile policies and system security policies in your SAP environment.

## Audience

---

This tutorial is suitable for those professionals who have a good understanding about SAP Basis tasks and a basic understanding of the system security. After completing this tutorial, you will find yourself at a moderate level of expertise in implementation of the security concepts in a SAP system.

## Prerequisites

---

Before you start with this tutorial, we assume that you are well-versed with SAP Basis activities – User Creations, Password Management, and RFC's. In addition, you should have a basic understanding of security terms in the Window and UNIX environment.

## Copyright & Disclaimer

---

© Copyright 2018 by Tutorials Point (I) Pvt. Ltd.

All the content and graphics published in this e-book are the property of Tutorials Point (I) Pvt. Ltd. The user of this e-book is prohibited to reuse, retain, copy, distribute or republish any contents or a part of contents of this e-book in any manner without written consent of the publisher.

We strive to update the contents of our website and tutorials as timely and as precisely as possible, however, the contents may contain inaccuracies or errors. Tutorials Point (I) Pvt. Ltd. provides no guarantee regarding the accuracy, timeliness or completeness of our website or its contents including this tutorial. If you discover any errors on our website or in this tutorial, please notify us at [contact@tutorialspoint.com](mailto:contact@tutorialspoint.com)

## Table of Contents

---

About the Tutorial.....	i
Audience .....	i
Prerequisites .....	i
Copyright & Disclaimer.....	i
Table of Contents .....	ii
 1. SAP SECURITY – OVERVIEW .....	 1
Why is Security Required?.....	1
 2. SAP SECURITY – USER AUTHENTICATION & MANAGEMENT .....	 3
Authentication Mechanism in a SAP System .....	3
User Management Tools in a SAP System .....	4
Password Policy .....	6
Illegal Passwords .....	8
Profile Parameters .....	9
 3. SAP SECURITY – NETWORK COMMUNICATION SECURITY.....	 15
Network Topology in a SAP System .....	15
SAP Network Services .....	16
Private Keys .....	17
 4. SAP SECURITY – PROTECTING STANDARD USERS.....	 19
How to See the List of Clients in a SAP System? .....	20
How to Change Password of a Standard User? .....	25
 5. SAP SECURITY – UN-AUTHORIZING LOGONS PROTECTIONS .....	 26
Logging off Idle Users .....	32

6.	SAP SECURITY – SYSTEM AUTHORIZATION CONCEPT .....	34
	User Types .....	34
	Creating a User .....	35
	Central User Administration (CUA) .....	38
	Protecting Specific Profiles in SAP .....	41
	PFCG.....	44
	Role Maintenance .....	44
	Creating Roles in PFCG .....	48
	Transporting and Distributing Roles .....	50
	Authorization Info System Transaction – SUIM .....	52
7.	SAP SECURITY – UNIX PLATFORM .....	55
8.	SAP SECURITY – WINDOWS PLATFORM.....	57
9.	SAP SECURITY – DATABASES.....	59
	Oracle Standard Users.....	59
	Password Management for DB Users .....	60
10.	SAP SECURITY – USER AUTHENTICATION & SINGLE SIGN-ON .....	62
	SAP Single Sign-On Concept .....	62
11.	SAP SECURITY – LOGON TICKETS .....	68

# 1. SAP Security – Overview

In a SAP Distributed Environment, there is always a need that you protect your critical information and data from unauthorized access. Human Errors, Incorrect Access Provisioning shouldn't allow unauthorized access to any system and there is a need to maintain and review the profile policies and system security policies in your SAP Environment.

To make the system secure, you should have good understanding of user access profiles, password policies, data encryption and authorization methods to be used in the system. You should regularly check **SAP System Landscape** and monitor all the changes that are made in configuration and access profiles.

The standard super users should be well-protected and user profile parameters and values should be set carefully to meet the system security requirements.

While communicating over a network, you should understand the network topology and network services should be reviewed and enabled after considerable checks. Data over the network should be well protected by using private keys.

## Why is Security Required?

---

To access the information in a distributed environment, there is a possibility that critical information and data is leaked to unauthorized access and system security is broken due to either – Lack of password policies, Standard super users are not well maintained, or any other reasons.

A few key reasons of breach of access in a SAP system are as follows:

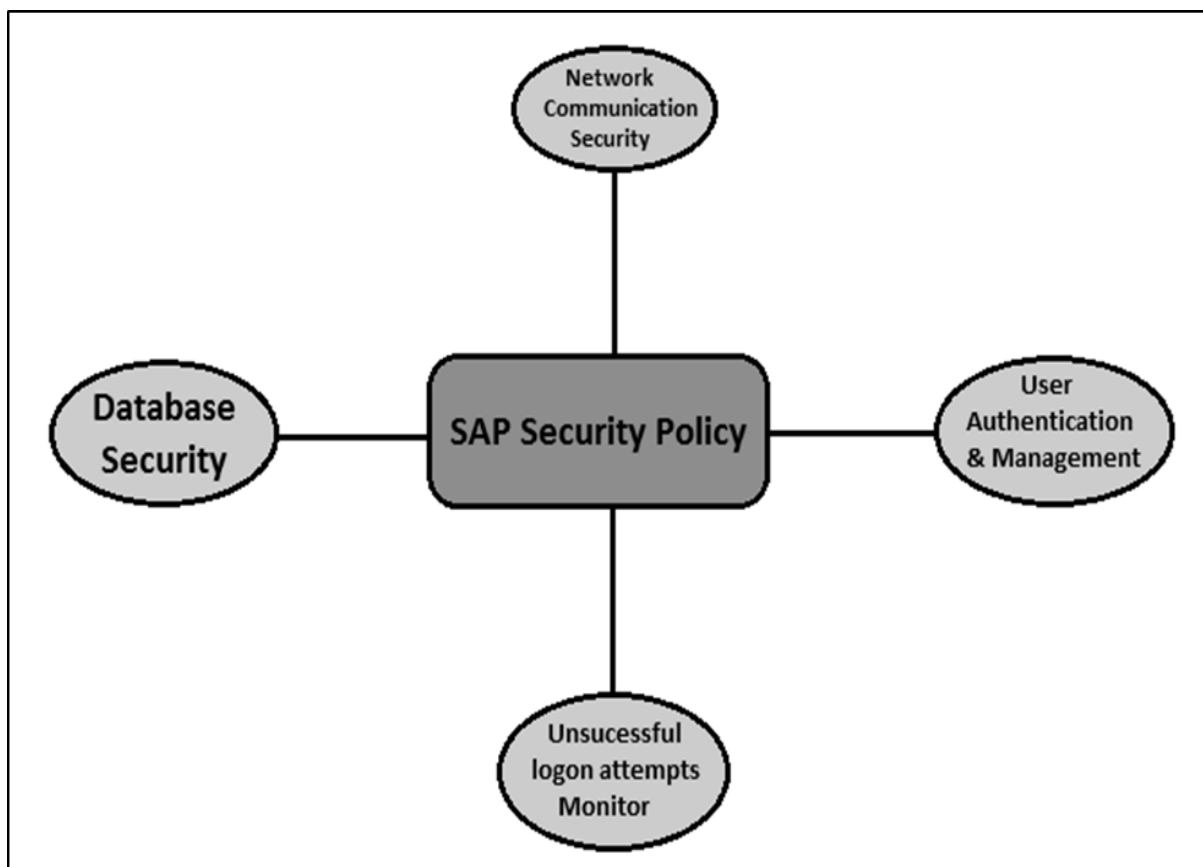
- Strong password policies are not maintained.
- Standard users, super user, DB users are not properly maintained and passwords are not changed regularly.
- Profile parameters are not correctly defined.
- Unsuccessful logon attempts are not monitored and idle user session end policies are not defined.
- Network Communication security is not considered while sending data over internet and no use of encryption keys.
- Database users are not maintained properly and no security measures are considered while setting up the information database.
- Single Sign-on's are not properly configured and maintained in a SAP environment.

To overcome all the above reasons there is a need that you define security policies in your SAP environment. Security parameters should be defined and password policies should be reviewed after regular time intervals.

The Database Security is one of the critical component of securing your SAP environment. So, there is a need that you manage your database users and see to it that passwords are well protected.

The following Security mechanism should be applied in the system to protect SAP Environment from any unauthorized access:

- User Authentication and Management
- Network Communication Security
- Protecting Standard Users and Super users
- Unsuccessful Logons Protections
- Profile parameters and password policies
- SAP System Security in Unix and Windows Platform
- Single Sign-On Concept



So, the security in SAP system is required in a distributed environment and you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. In a SAP system, human errors, negligence, or attempted manipulation on the system can result in loss of critical information.

## 2. SAP Security – User Authentication & Management

If an unauthorized user can access SAP system under a known authorized user and can make configuration changes and manipulate system configuration and key policies. If an authorized user has access to important data and information of a system, then that user can also access other critical information as well. This enhances the use of secure authentication to protect the Availability, Integrity and Privacy of a User System.

### Authentication Mechanism in a SAP System

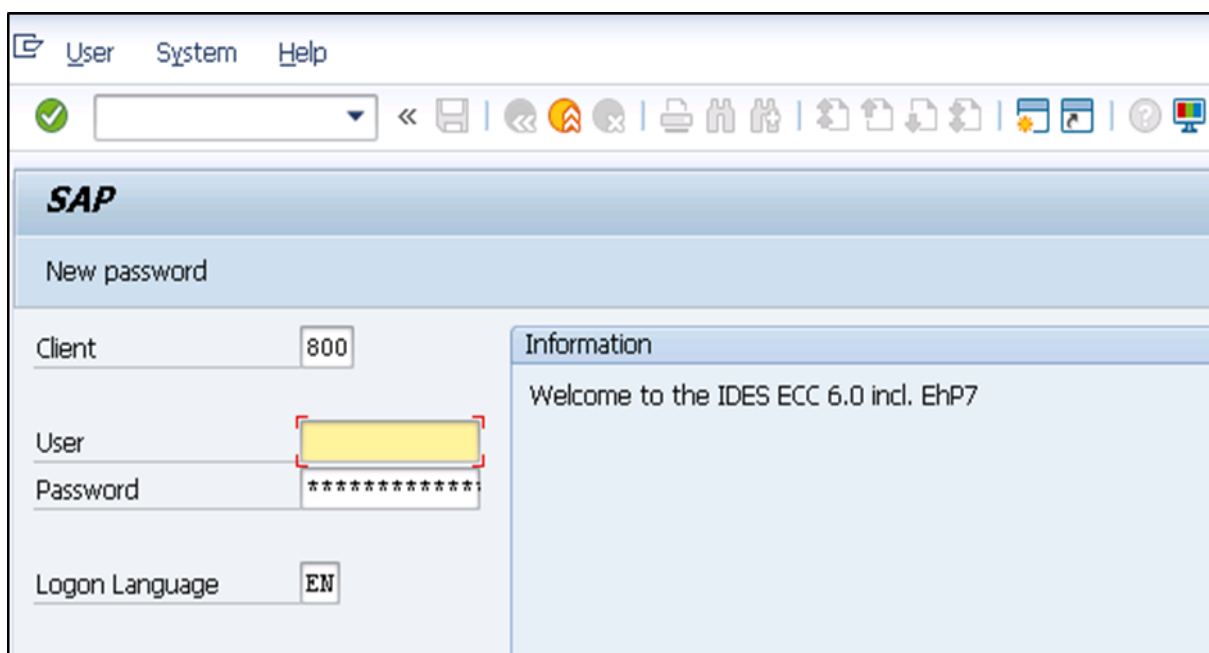
Authentication mechanism defines the way you access your SAP system. There are various authentication methods that are provided:

- User ID's and user management tools
- Secure Network Communication
- SAP Logon Tickets
- X.509 Client Certificates

### User ID's and User Management Tools

Most common method of authentication in a SAP system is by using the username and password to login. The User ID's to login are created by the SAP Administrator. To provide secure authentication mechanism via the username and password, there is a need to define password policies that doesn't allow users to set easy predicted password.

SAP provides various default parameters that you should set to define password policies- password length, password complexity, default password change, etc.





## User Management Tools in a SAP System

**SAP NetWeaver System** provides various user management tools that can be used to effectively manage users in your environment. They provide very strong authentication method for both type of NetWeaver Application servers – Java and ABAP.

Some of the most common User Management Tools are:

### User Management for ABAP Application Server (Transaction Code: SU01)

You can use user management Transaction-Code SU01 to maintain users in your ABAP based Application Servers.

### SAP NetWeaver Identity Management

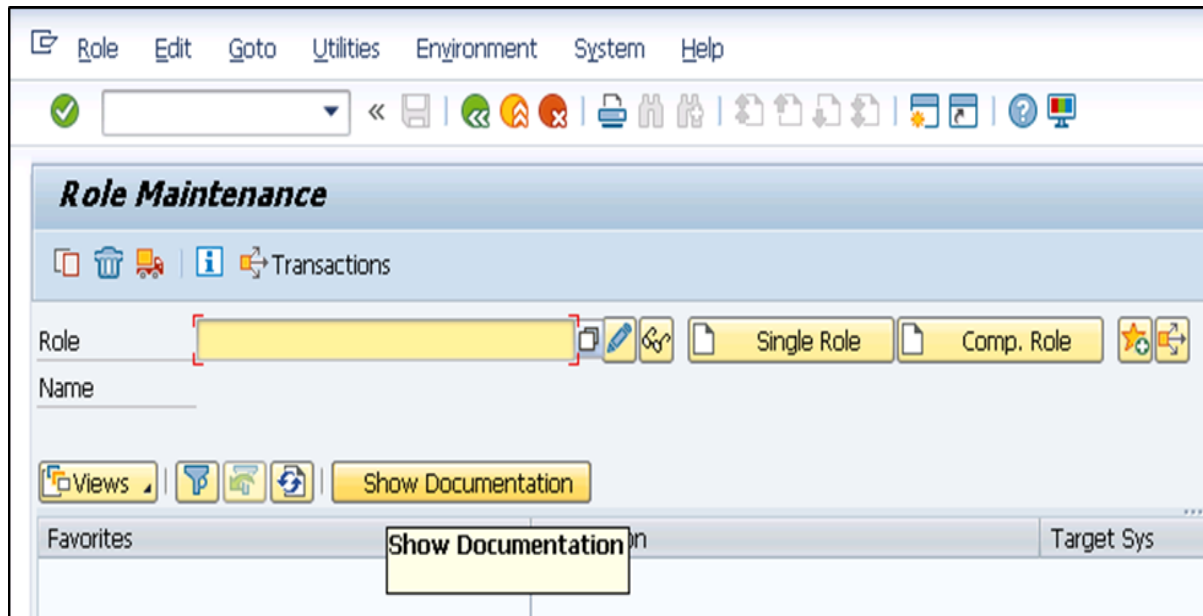
You can use SAP NetWeaver Identity Management for user management as well as for managing roles and role assignments in your SAP environment.



## PFCG Roles

You can use profile generator PFCG to create roles and assign authorizations to users in ABAP based systems.

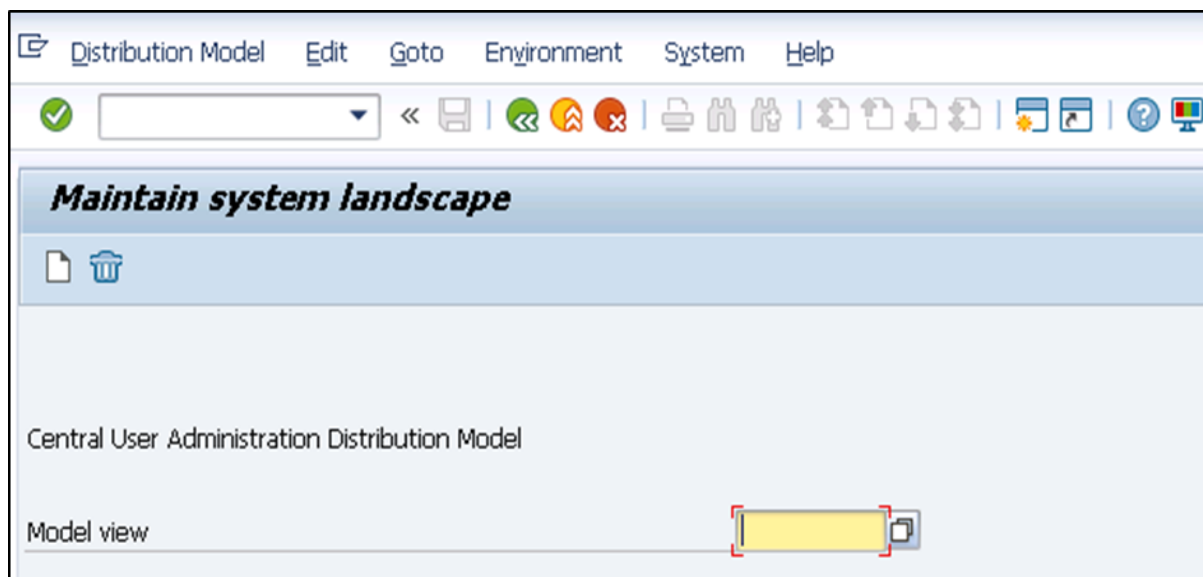
**Transaction Code:** PFCG



## Central User Administration

You can use CUA to maintain users for multiple ABAP-based systems. You can also sync it with your directory servers. Using this tool, you can manage all the user master record centrally from the client of the system.

**Transaction Code:** SCUA and create distribution model.



## User Management Engine UME

You can use UME roles to control the user authorization in the system. An administrator can use actions which represent the smallest entity of UME role that a user can use to build access rights.

You can open UME administration console using SAP NetWeaver Administrator option.

## Password Policy

---

A password policy is defined as a set of instructions that a user must follow to improve system security by using strong passwords and by using them properly. In many organizations, password policy is shared as a part of security awareness training and it is mandatory for users to maintain the policy for security of critical systems and information in an organization.

Using password policy in a SAP system, an administrator can setup system users to deploy strong passwords that are not easy to break. This also helps to change the password at the regular time intervals for system security.

The following password policies are commonly used in a SAP System:

### Default/Initial Password Change


This allows the users to change the initial password immediately when used for the first time.

### Password Length


In a SAP system, the minimum length for passwords in SAP Systems is 3 by default. This value can be changed using profile parameter and maximum length that is allowed is 8.


**Transaction Code:** RZ11

**Parameter Name:** login/min\_password\_lng

Maintain Profile Parameters	
	
Metadata for Parameter login/min_password_lng	
Description	Value
Name	login/min_password_lng
Type	Integer Interval
Further Selection Criteria	Interval [3,40]
Unit	
Parameter Group	Login
Parameter Description	Minimum Password Length
CSN Component	BC-SEC-LGN
System-Wide Parameter	Yes
Dynamic Parameter	No
Vector Parameter	No
Has Subparameters	No
Check Function Exists	No
Current Value of Parameter login/min_password_lng	
Expansion Level	Value
Kernel Default	6
Standard Profile	6
Instance Profile	6
Current Value	6

You can click on documentation of the profile parameter for this policy and you can see the detailed documentation as from SAP as follows:

 Performance Assistant



## Parameter

login/min\_password\_lng

## Short text

Minimum password length

## Parameter Description

This parameter specifies the minimum length of the logon password. The password must have at least three characters, however the administrator can specify a greater minimum length. This setting applies when new passwords are assigned and when existing passwords are changed or reset.

## Application Area

Logon

**Parameter:** login/min\_password\_lng

**Short text:** Minimum password length

**Parameter Description:** This parameter specifies the minimum length of the logon password. The password must have at least three characters. However, the administrator can specify a greater minimum length. This setting applies when new passwords are assigned and when existing passwords are changed or reset.

**Application Area:** Logon

**Parameter Unit:** Number of characters (alphanumeric)

**Default Value:** 6

**Who is permitted to make changes?** Customer

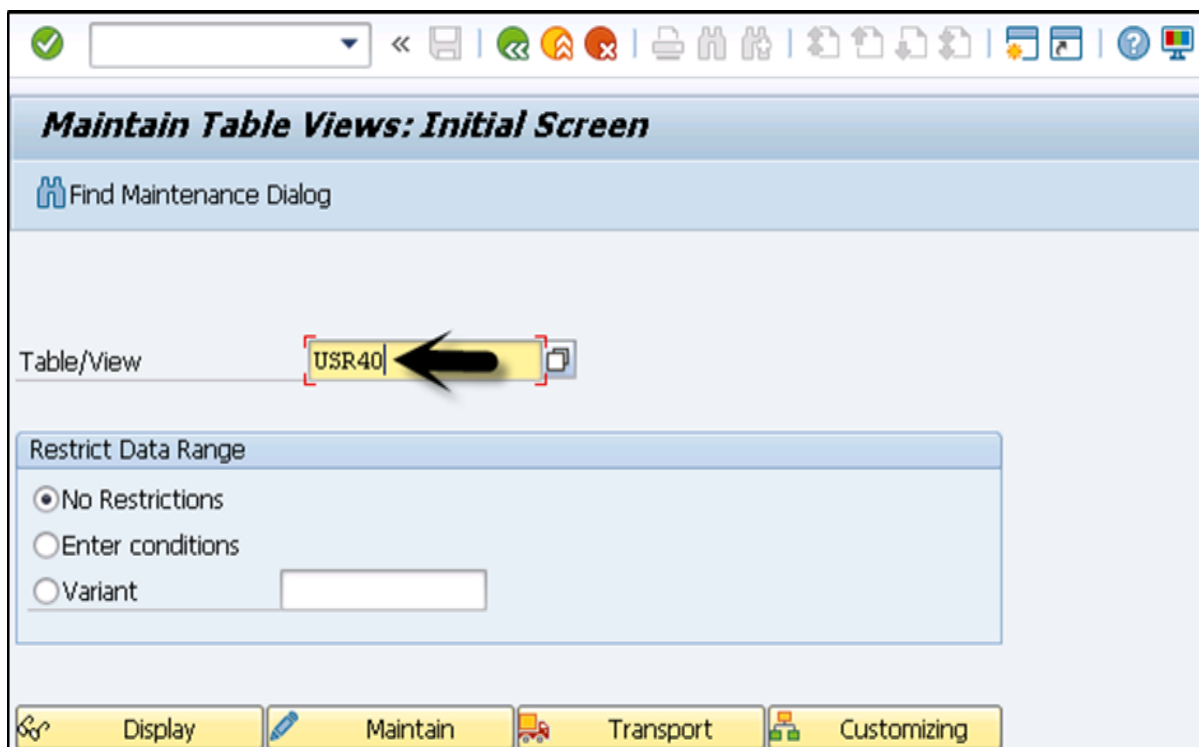
**Operating System Restrictions:** None

**Database System Restrictions:** None

## Illegal Passwords

You cannot select the first character of any password as a question mark (?) or an exclamation mark (!). You can also add the other characters that you want to restrict in the illegal password table.

**Transaction Code:** SM30 Table Name: USR40



Once you enter the table – **USR40** and click on **Display** at the top, it will show you the list of all the impermissible passwords.

**Change View "Table for illegal passwords": Overview**

New Entries

Password Patt./Indiv. Value	Case-Sens?

Once you click on **New Entries**, you can enter the new values to this table and also select the case sensitive check box.

**Change View "Table for illegal passwords": Overview**

New Entries

Password Patt./Indiv. Value	Case-Sens?

## Password Pattern

You can also set that the first three characters of the password cannot appear in the same order as part of the user name. Different password patterns that can be restricted using password policy include:

- The first three characters cannot all be the same.
- The first three characters cannot include space characters.
- The password cannot be PASS or SAP.

## Password Change

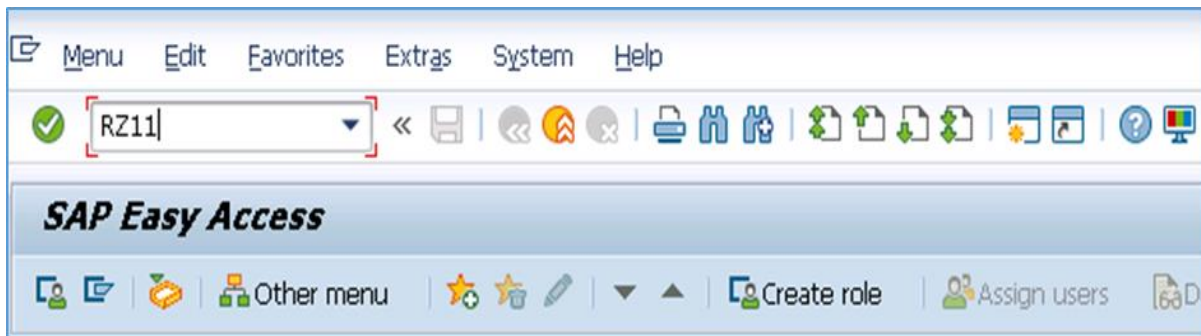
In this policy, a user can be allowed to change his or her password almost once a day, but an administrator can reset a user's password as often as necessary.

A user shouldn't be allowed to reuse the last five passwords. However, an administrator can reset the password that is used by a user previously.

## Profile Parameters

There are different profile parameters that you can define in a SAP system for user management and password policy.

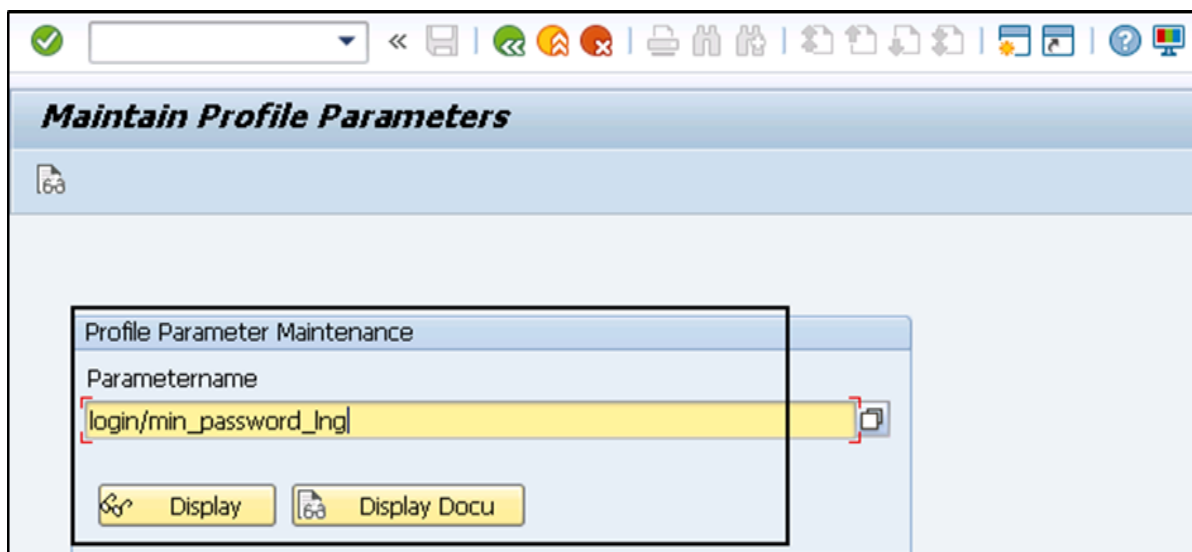
In a SAP system, you can display the documentation for each profile parameter by going to **Tools → CCMS → Configuration → Profile Maintenance** (Transaction: RZ11). Enter the parameter name and click on **Display**.



In the next window that shows up, you must enter the parameter name, you can see 2 options:

**Display:** To display the value of parameters in SAP system.


**Display Docu:** To display SAP documentation for that parameter.



When you click on the Display button, you will be moved to **Maintain Profile Parameter** screen. You can see the following details:


- Name
- Type
- Selection Criteria
- Parameter Group
- Parameter Description and many more

At the bottom, you have current value of parameter **login/min\_password\_lng**.

Maintain Profile Parameters	
	
Metadata for Parameter login/min_password_lng	
Description	Value
Name	login/min_password_lng
Type	Integer Interval
Further Selection Criteria	Interval [3,40]
Unit	
Parameter Group	Login
Parameter Description	Minimum Password Length
CSN Component	BC-SEC-LGN
System-Wide Parameter	Yes
Dynamic Parameter	No
Vector Parameter	No
Has Subparameters	No
Check Function Exists	No
Current Value of Parameter login/min_password_lng	
Expansion Level	Value
Kernel Default	6
Standard Profile	6
Instance Profile	6
Current Value	6

When you click on **Display Doc** option, it will display SAP documentation for the parameter.

Performance Assistant



## Parameter

login/min\_password\_lng

## Short text

Minimum password length

## Parameter Description

This parameter specifies the minimum length of the logon password. The password must have at least three characters, however the administrator can specify a greater minimum length. This setting applies when new passwords are assigned and when existing passwords are changed or reset.

## Application Area

Logon

## Parameter Unit

Number of characters (alphanumeric)



## Parameter Description

This parameter specifies the minimum length of the logon password. The password must have at least three characters. However, the administrator can specify a greater minimum length. This setting applies when new passwords are assigned and when existing passwords are changed or reset.

Each parameter has a default value, permitted value as below:

Parameter	Description	Default	Permitted value
login/min_password_lng	Minimum length	3	3 - 8
login/password_expiration_time	Number of days after which a password must be changed.	0 (no limit)	any numerical value

There are different password parameters in a SAP system. You can enter each parameter in the **RZ11** transaction and can view the documentation.

- login/min\_password\_diff
- login/min\_password\_digits
- login/min\_password\_letters
- login/min\_password\_specials
- login/min\_password\_lowercase
- login/min\_password\_uppercase
- login/disable\_password\_logon
- login/password\_charset
- login/password\_downwards\_compatibility
- login/password\_compliance\_to\_current\_policy

To change the Parameter value, run **Transaction RZ10** and select the Profile as shown below:

- **Multiple application servers:** Use DEFAULT profile.
- **Single Application servers:** Use Instance Profile.

Select **Extended Maintenance** and click **Display**.

Select the parameter that you want to change and click on **Parameter** at the top.

Parameter Name	Parameter value
SAPDEHOST	BODS
dbms/type	mss
dbms/mss/server	BODS
dbms/mss/dbname	EH7
dbms/mss/schema	eh7
SAPSYSTEMNAME	EH7
SAPGLOBALHOST	BODS
system/type	ABAP
rsdb/ssfs_connect	0
rdisp/mshost	BODS
rdisp/msserv	sapmsEH7
rdisp/msserv_internal	3901
enque/process_location	REMOTESA
enque/serverhost	BODS
enque/serverinst	01
is/HTTP/show_detailed_errors	FALSE
icf/user_recheck	1
icm/HTTP/ASJava/disable_url_session_trackin	TRUE
service/protectedwebmethods	SDEFAULT
rsec/ssfs_datapath	\$(DIR_GLOBAL)\$(DIR_SEP)security\$(DIR_SEP)rsecssfs\$(DIR_SEP)data
rsec/ssfs_keypath	\$(DIR_GLOBAL)\$(DIR_SEP)security\$(DIR_SEP)rsecssfs\$(DIR_SEP)key
gw/acl_mode	1
gw/sec_info	\$(DIR_GLOBAL)\$(DIR_SEP)secinfo\$(FT_DAT)
login/password_downwards_compatibility	0
login/system_client	001
rdisp/TRACE	1

When you click on the **Parameter** tab, you can change the value of parameter in new window. You can also create the new parameter by clicking on **Create (F5)**.

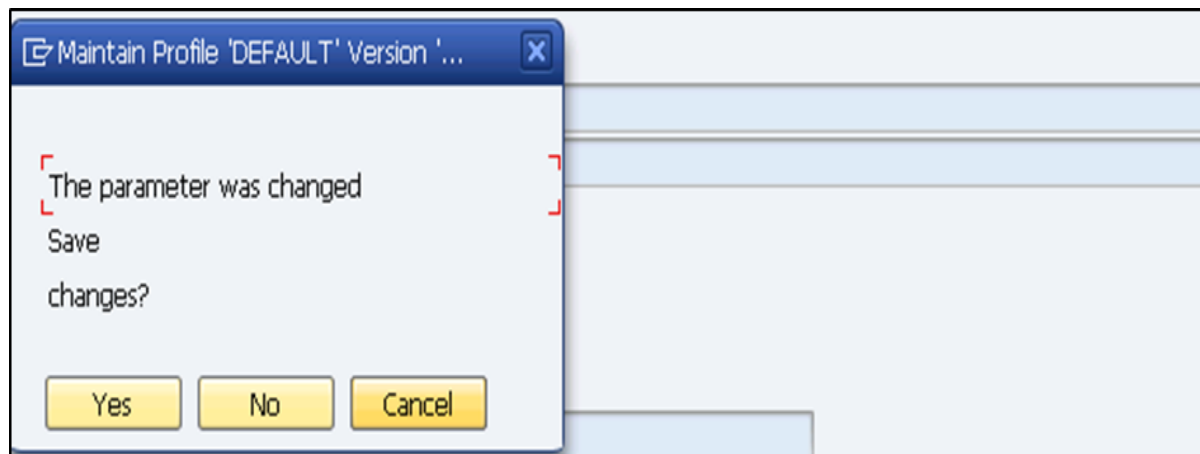
You can also see the status of the parameter in this window. Type the parameter value and click on **Copy**.

The screenshot shows the SAP Security parameter configuration interface. At the top, there are navigation icons (Copy, Line, Line) and buttons for 'PARAM+' and 'PARAM-'. The main area contains a table with the following data:

Parameter name:	Status	Seq. no.
login/system_client	Active	25

Below the table, there is a 'Parameter val.' field with the value '001' highlighted in yellow. Further down, there are fields for 'Unsubstituted standard value:' and 'Substituted standard value:', both containing '001'. At the bottom, there is a 'Comment:' field with a '#' symbol.

You will be prompted to save when you exit the screen. Click on **Yes** to save the parameter value.



End of ebook preview

If you liked what you saw...

Buy it from our store @ **<https://store.tutorialspoint.com>**